MW

Notice of Allowability	Application No.	Applicant(s)	
	09/378,226	RIGGINS, MARK D.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/15/07*.

2. ☒ The allowed claim(s) is/are *1-30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. This is in response to the amendment filed on 15 June 2007.

2. Claims 1-30 are pending in the application.

3. Claims 1-30 have been allowed.

Response to Amendment

4. The examiner approves the amendment made to the claims. No new matter has been added to the claims.

Response to Arguments

5. Applicant's arguments, see pages 10-17, filed 15 June 2007, with respect to claims 1-30 have been fully considered and are persuasive. The rejection of the claims has been withdrawn.

Allowable Subject Matter

6. Claims 1-30 are allowed.

The following is an examiner's statement of reasons for allowance:

The current application is directed towards a system and method to distribute the task of decryption between a server and a client. To encrypt data, the client generates an encryption/decryption key. Namely, a user interface obtains a password, generally from a user. A hint generator generates a hint. A key generator generates the key based on the password and the hint. In one embodiment, the key generator hashes the password to generate a first secret, hashes the first secret to generate a second secret, hashes the first secret with the hint to generate an intermediate index, and hashes the second secret and the intermediate index to generate the key. An encryption engine can then use the key to encrypt data. The client then sends the encrypted data and possibly the hint for storage on the server. To decrypt the data, the key must

be determined. Accordingly, the server knows some information and the user knows some information for decrypting the data. To generate the key, the decrypting client must first obtain rights to retrieve the hint from the server and must obtain the password from the user. Increased level of security is achieved.

The closest prior art to claims 1-2, 4-6, and 8-19 was Grawrock U.S. Patent No. 6,360,322 B1 (hereinafter Grawrock). Grawrock is directed towards a method of securely and automatically authenticating a user. Bona fides are entered for a user, hashed, and stored at an authenticating entity, remote from the user's computer. When a user forgets his/her password, the user enters his/her bona fides, which are again hashed on the user's system, and then securely transmitted to the authenticating entity. The authenticating entity compares the received, hashed bona fides to those previously stored at the authenticating entity. If the comparison shows that the values match or otherwise appropriately correlate, the user will be authenticated. The user will then be provided with the means to access his/her encrypted data. In other words, once authenticated the authenticating entity will automatically provide the user and/or the user's computer with an access key, in one embodiment, allowing the user to access his/her encrypted data.

However, there are differences between the current application and the Grawrock reference. With respect to independent claims 1 and 8, Grawrock does not disclose the elements set forth in claims 1 and 8, which include, inter alia, (i) "performing a hashing algorithm on the hint and the password to generate a key", (ii) "encrypting data using the key", and (iii) "sending the encrypted data to a server for storage". Grawrock discloses that only the password is hashed rather than "performing a hashing algorithm on the hint and the password" as recited in claims 1

and 8. Grawrock states that the "hash of the entered user password is taken" [column 6, lines 54-55] but there is no mention in Grawrock that another item (e.g., "question") is also hashed. In fact, as shown in FIG. 2 of Grawrock, the "hash function 262" has only the "user password" as its input. Thus, Grawrock does not disclose "performing a hashing algorithm on the hint and the password" as recited in claims 1 and 8. Grawrock discloses that "all $File_i$ are encrypted with a K_{fi}", but " K_{fi}" is not a "key" generated by "performing a hashing algorithm on the hint and the password" as set forth in claims 1 and 8. Thus, Grawrock does not disclose "encrypting data using the key" as recited in claims 1 and 8 where the key is generated by "performing a hashing algorithm on the hint and the password." Grawrock discloses sending an encrypted "K_{acc2}" to "authenticating entity 299"; however, "K_{acc2}" is an "access key" rather than data. In addition, Grawrock discloses that the "authenticating entity 299" sends back to the "computer system 200" the " K_{acc2}" which, as stated earlier, is an "access key" rather than data. Thus, Grawrock does not disclose "sending the encrypted data to a server for storage" as set forth in claims 1 and 8.

With respect to independent claim 4, Grawrock does not disclose the elements set forth in claim 4, which include, inter alia, (i) "a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key", (ii) "an encryption engine coupled to the key generator for encrypting data using the key", and (iii) "a communications module coupled to the engine for sending the encrypted data and the hint to a server for storage". For reasons similar to those provided earlier with respect to claims 1 and 8, claim 4 is also patentable over Grawrock. Claims 5-6 depend from claim 4 and so these two claims are also patentable over Grawrock. With respect to independent claim 11, Grawrock does not disclose the elements set forth in claim 11, which include, inter alia, (i) "receiving a request to store encrypted data from a

client", (ii) "sending an encryption downloadable for deriving a key to encrypt data to the client", and (iii) "receiving encrypted data that was encrypted by the encryption downloadable from the client". Grawrock discloses encrypting "file data", but there is no mention of "receiving a request ... from a client" as set forth in claim 11. Grawrock discloses a "file encryption key K_{fi} " rather than an "encryption downloadable for deriving a key" as set forth in claim 11. Grawrock does not disclose "sending an encryption downloadable to the client" as set forth in claim 11; in fact, it does not disclose sending anything to a client since Grawrock does not disclose a client-server system. Grawrock discloses encrypting the access key " K_{fi} "; however, this portion nor anywhere else in Grawrock discloses "receiving encrypted data ... from the client" as set forth in claim 11. With respect to independent claim 12, Grawrock does not disclose the elements set forth in claim 12, which include, inter alia, "a web server for interfacing with a client, for sending the encryption downloadable to the client, and for receiving encrypted data that was encrypted by the encryption downloadable from the client." Grawrock discloses encrypting the "encryption key K_{fi} " using the "encrypting unit 218"; however, this portion does not disclose a "web server", nor receiving "encrypted data .. from the client" as set forth in claim 12. With respect to independent claims 13, 15, and 16, Grawrock does not disclose the elements set forth in these claims, which include, inter alia, "sending encrypted data and a hint corresponding to the encrypted data from a server to a client" and "performing a hashing algorithm on the password and the hint at the client to generate a key for decrypting the encrypted data". Grawrock discloses sending an "OT private key" and "various identifying information" to the "authenticating entity"; however, the cited portion does not disclose "sending encrypted data . . . to a client" as set forth in claims 13, 15, and 16. With respect to

the "performing" element, for the reasons provided earlier with respect to claims 1 and 8, Grawrock does not disclose this element. Claim 14 depends from claim 13, and claims 17-18 depend from claim 16. Thus, for the reasons provided earlier with respect to the independent claims, these dependent claims are also patentable over Grawrock. With respect to independent claim 19, Grawrock does not disclose the elements set forth in claim 19, which include, inter alia, "sending a decryption downloadable for deriving a key from a password and a hint to a client". Grawrock discloses sending an "OT private key" and "various identifying information" to the "authenticating entity 299"; however, the cited portion does not disclose that the "authenticating entity 299" uses a "password" and no "password" is ever sent to the "authenticating entity 299", and thus the "authenticating entity 299" is not sent "a decryption downloadable for deriving a key from a password and a hint" as set forth in claim 19.

The closest prior art to claims 3, 7 and 20-30 was Challener et al U.S. Patent No. 6,470,454 B1 (hereinafter Challener). Challener is directed towards a method and apparatus for facilitating the generation and use of computer system configuration passwords which can be utilized in an enterprise or organization to allow authorized users having knowledge of the password associated with a particular data processing system to make and change configuration decisions, but which prevents unauthorized users from making and changing such configuration decisions. In the preferred embodiment, a unique identifier (such as a serial number) and an enterprise secret key are supplied to a one-way cryptographic hash function in order to generate the configuration passwords that are unique to each data processing system of the plurality of data processing system of the enterprise or organization.

With respect to independent claim 3, the Applicant submits that Challener does not disclose the elements set forth in claim 3, which include, inter alia, (i) "performing a hashing algorithm on the hint and the password to generate a key, wherein the step of performing a hashing algorithm includes hashing the password to derive a first secret, hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key", (ii) "encrypting data using the key", and (iii) "sending the encrypted data to a server for storage". Challener discloses generating a "computer system configuration password" by obtaining the computer's serial number and a "relatively secret key" known only to the support organization, and these two items are concatenated together and then hashed to generate the password. Challener does not disclose, inter alia, "hashing the password to derive a first secret" as set forth in claim 3 because Challener discloses that the hashing function is performed to generate the password but the password is not one of the items that is hashed. In addition, Challener discloses that the "relatively secret key" is obtained from the support organization, rather than "derive a first secret" by hashing the password as set forth in claim 3. Also, Challener discloses performing only a single hashing function on the concatenation of the password and the "relatively secret key", but does not disclose performing multiple hash functions such as, e.g., "hashing the first secret to derive a second secret", "hashing the hint and the first secret to generate an intermediate index", and "hashing the intermediate index and the second secret" as set forth in claim 3. In addition, Challener discloses that the hashing function generates a "password", rather than generate the "key", the "intermediate index", the "second secret", or the "first secret" as set forth in claim 3. Challener discloses obtaining the "computer's serial

number" (this is not encrypted) from the computer user, rather than "sending the encrypted data to a server for storage" as set forth in claim 3. With respect to independent claim 7, for similar reasons provided with respect to claim 3, Challener does not disclose the elements set forth in claim 7, which include, inter alia, (i) "a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key wherein the key generator hashes the password to derive a first secret, hashes the first secret to derive a second secret, hashes the hint and the first secret to generate an intermediate index, and hashes the intermediate index and the second secret to generate the key", (ii) "an encryption engine coupled to the key generator for encrypting data using the key", and (iii) "a communications module coupled to the engine for sending the encrypted data to a server for storage". With respect to independent claim 20, Challener does not disclose the elements set forth in claim 20, which include, inter alia, (i) "a decryption downloadable for deriving a key by hashing at least one of a password and a hint", (ii) "encrypted data", and (iii) "a web server for interfacing with a client, and for sending the decryption downloadable, the encrypted data and the hint to the client". For (i), Challener discloses deriving a "password", rather than "a decryption downloadable for deriving a key by hashing at least one of a password and a hint" as set forth in claim 20. For (ii), Challener does not disclose "encrypted data". For (iii), Challener discloses that the "consultant" performs the hashing function at his computer and the only item received/sent from another entity is the "computer's serial number" (this number is not encrypted) which is obtained from the computer user. However, the computer user is not a client and thus at least for this reason, Challener does not disclose "a web server for interfacing with a client, and for sending the decryption downloadable, the encrypted data and the hint to the client". With respect

to independent claims 21 and 26, Challener does not disclose the elements set forth in claims 21 and 26, which include, inter alia, (i) "deriving a first secret from the password", (ii) "deriving an intermediate index from the first secret and the hint", and (iii) "sending the intermediate index to the server". Challener discloses generating a password using the computer's serial number and a "relatively secret key", which is almost the opposite of "deriving a first secret from the password" as set forth in claims 21 and 26. Challener discloses generating a password using the computer's serial number and a "relatively secret key", rather than "deriving an intermediate index from the first secret and the hint" as set forth in claims 21 and 26. Challener discloses receiving the computer's serial number from the computer user, rather than "sending the intermediate index to the server" as set forth in claims 21 and 26. For the foregoing reasons, claims 21 and 26 are patentable over Challener. Claims 22-23 depend from claim 21, and claims 27-28 depend from claim 26. Thus, these dependent claims are also patentable over Challener. With respect to independent claim 24, Challener does not disclose the elements set forth in claim 24, which include, inter alia, (i) "an index generator coupled to the user interface for generating an intermediate index from a hint received from a server and a secret derived from the password", and (ii) "a communications engine coupled to the index generator for sending the intermediate index to the server." Challener discloses generating a password using the computer's serial number and a "relatively secret key", rather than an "index generator" that generates an intermediate index using in part "a secret derived from the password" as set forth in claim 24. Challener discloses receiving the computer's serial number from the computer user, rather than "a communications engine coupled to the index generator for sending the intermediate index to the server" as set forth in claim 24. For the foregoing reasons, claim

24 is patentable over Challener. Claim 25 depends from claim 24, and thus, it is also patentable over Challener. With respect to independent claims 29, Challener does not disclose the elements set forth in claims 29, which include, inter alia, (i) "receiving an indication of encrypted data to be decrypted", (ii) "transmitting to a client a hint corresponding to the indication, and a decryption downloadable for deriving an intermediate index from a password and the hint", (iii) "receiving the intermediate index from the client", and (iv) "deriving a decryption key from a second secret corresponding to the user and the intermediate index." There is no indication in Challener that any data is ever encrypted. Challener discloses deriving a password rather than "deriving an intermediate index from a password and the hint" as set forth in claim 29. Challener discloses receiving the computer's serial number from the computer user, rather than "receiving the intermediate index from the client" as set forth in claim 29. Challener discloses generating a password using the computer's serial number and a "relatively secret key", however, it does not disclose "deriving a decryption key" or the "second secret" set forth in claim 29. For the foregoing reasons, claim 29 is patentable over Challener. With respect to independent claim 30, Challener does not disclose the elements set forth in claim 30, which include, inter alia, (i) "a decryption downloadable for generating an intermediate index from a password and a hint", (ii) "a web server for receiving an indication of encrypted data to be decrypted, for transmitting the decryption downloadable and a hint corresponding to the indication to a client, and for receiving an intermediate index from the client", and (iii) "a server-resident module for deriving a key for decrypting the encrypted data from the second secret and the intermediate index." Challener discloses generating a password using the computer's serial number and a "relatively secret key", rather than "a decryption downloadable

for generating an intermediate index from a password and a hint" as set forth in claim 30. Challener discloses receiving the computer's serial number from the computer user in order to generate the password, but Challener does not disclose generating an intermediate index. The "computer user" of Challener is not a "web server" set forth in claim 30, nor does Challener disclose, inter alia, the "intermediate index" set forth in claim 30. Challener discloses generating a "password"; however, it does not disclose a "server-resident module for deriving a key", "encrypted data", "second secret", and "intermediate index" as set forth in claim 30.

Any claims not directly addressed are allowed on the virtue of their dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy AM
July 13, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100